(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 March 2005 (31.03.2005)

PCT

(10) International Publication Number
WO 2005/029272 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/030548

(22) International Filing Date:
15 September 2004 (15.09.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/503,511 15 September 2003 (15.09.2003) US

(71) Applicant *(for all designated States except US)*: **ACRES GAMING INCORPORATED** [US/US]; 7115 Amigo Street, Suite 150, Las Vegas, NV 89119 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FORBES, Mark, G.** [US/US]; 815 Northwest 9th Street, Corvallis, OR 97330 (US). **RIEGELMANN, Robert, A.** [US/US]; 815 Northwest 9th Street, Corvallis, OR 97330 (US).

(74) Agents: **SCHAFFER, Scott, A.** et al.; Marger Johnson & McCollom P.C., 1030 SW Morrison St., Portland, OR 97205 (US).

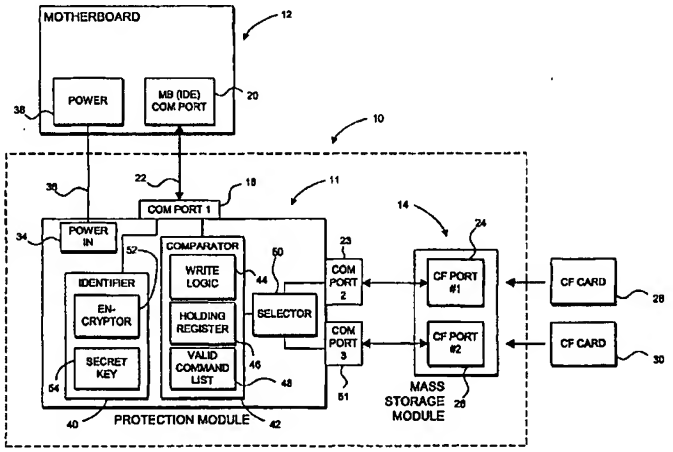
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND DEVICE FOR DATA PROTECTION AND SECURITY IN A GAMING MACHINE



(57) Abstract: A method and apparatus is described for the protection of data in a mass storage device used for gaming applications. The device works in conjunction with the industry-standard hard disk interface port commonly found on a personal computer motherboard, and an off-the-shelf standard mass storage device. During operation, the protection device intercepts each command packet sent to the storage device, and passes through only those commands which are approved for use. The device may answer certain commands on behalf of the storage device, to supply default responses to non-approved command requests. The device also responds to certain other commands on its own, providing a means of verifying its continued presence to defeat attempts to bypass or remove it. To defeat attempts to copy or mimic its operation, a standard cryptographic algorithm is implemented internally with a secret key, and the entire device is protected against data extraction that could reveal the key.

WO 2005/029272 A2

METHOD AND DEVICE FOR DATA PROTECTION AND SECURITY IN A GAMING MACHINE

BACKGROUND OF THE INVENTION

1. Field of the Invention.

The invention relates to a mass storage data protection device, and more particularly to a protection device for use with an industry-standard mass storage device having no other reliable method of preventing unauthorized alteration of the stored data while operating inside a gaming machine.

2. Description of the Prior Art.

Gaming machines are operated within a tightly regulated industry, and historical precedent has held that critical operating code for such machines should be stored in non-alterable memory to defeat tampering. Media such as EPROM or masked ROM were considered acceptable, since these could not be rewritten in-system, and their contents could be verified in the field to insure that no tampering had occurred. While reasonably secure from tampering, such media are limited in the amount of data they can hold.

As data requirements for modern games expand, larger data storage devices are required. While it is technically possible to produce large arrays of ROM or EPROM storage devices, such arrays are custom-produced, expensive and unwieldy. At the same time, large memory arrays of re-writeable "Flash" memory are now available in standard packages with a standardized interface. Flash memories, however, pose an unacceptable security risk when used in conjunction with gaming machines. Though these devices ("Compact Flash Cards") can store large amounts of data and can be rewritten repeatedly, they lack a built-in means for preventing rewriting of the data by either a rogue program or a deliberate programmatic attack.

Data protection schemes have been described before, but they suffer from various limitations or are inapplicable to the gaming machine requirements. U.S. Reissue Patent Re 33,328 (Director) teaches a method using separate and

independent control and data buses, but such methods are inappropriate for use with Compact Flash Cards.

Others have taken somewhat different approaches to secure memory. Patents issued to Stutz (U.S. Patent No. 5,668,973), Ishimoto (U.S. Patent No. 6,101,586) and others describe methods of protecting specific areas of memory from inadvertent overwriting in connection with a computer processor, but these methods do not address the selective permission or denial of commands to a memory device such as a Compact Flash (CF) card using a packet-based command sequence.

U.S. Patent No. 6,488,581 (Stockdale) teaches a method using a protection device, but this method relies on a monitoring means which detects an illegal command and asserts a reset signal to abort the operation of the mass storage device before data can be written to the storage device. It also generates a fault signal output to the gaming machine which interrupts the normal operation of the machine. Stockdale, however, provides no method for verifying the presence of the security device to prevent bypass and/or removal from the gaming machine.

Accordingly, the need still exists for a device and method that can prevent alteration of the data stored in a CF card while it is operating as part of a gaming machine, with a means for verification of the presence of the protection device and a means for determining whether the protection device has been tampered with.

SUMMARY OF THE INVENTION

It is therefore an object of the invention to provide a means of protecting the data in a CF card from alteration while it is connected to a gaming machine.

Another object of the invention is to provide a means for verifying the continued presence of the protection device, in a way that cannot easily be duplicated by an attacker.

A further object of the invention is to provide a means for verifying the internal integrity of the protection device, such that regulatory authorities or other privileged entities may confirm that the protection device contains the same

algorithms and internal constructs disclosed to them by the manufacturer of the device.

Still another object of the invention is to provide a means of terminating the operation of the gaming machine in the event that an illegal command is received by the protection device.

A method and apparatus is described for the protection of data in a mass storage device used for gaming applications. The device works in conjunction with the industry-standard hard disk interface port commonly found on a personal computer motherboard, and an off-the-shelf standard mass storage device. During operation, the protection device intercepts each command packet sent to the storage device, and passes through only those commands which are approved for use. The device may answer certain commands on behalf of the storage device, to supply default responses to non-approved command requests. The device also responds to certain other commands on its own, providing a means of verifying its continued presence to defeat attempts to bypass or remove it. To defeat attempts to copy or mimic its operation, a standard cryptographic algorithm is implemented internally with a secret key, and the entire device is protected against data extraction that could reveal the key.

The foregoing and other objects, features and advantages of the invention will become more readily apparent from the following detailed description of a preferred embodiment of the invention that proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a protection device integrated within a mass data storage system and configured according to a preferred embodiment of the invention.

FIG. 2 is a flow diagram illustrating operation of the protection device of FIG. 1 according to a preferred embodiment.

FIG. 3 is a block diagram illustrating operation of the protection device according to another aspect of the invention.

DETAILED DESCRIPTION

FIG. 1 illustrates an implementation of the preferred embodiment of the protection device 10 coupled to motherboard 12 and including a protection module and mass storage unit 14 incorporating two mass storage devices 24, 26. The figure illustrates but one means of reducing this invention to practice, as will be apparent to those skilled in the art.

The first communication port 18 is implemented as a connector which mates with a hard disk drive controller port 20 commonly found on personal computer motherboards, known generically as the "IDE port". This port supplies a 16-bit bidirectional data bus along line 22, as well as some address and control signals suitable for communicating with a mass storage device, such as an IDE hard disk drive, through a second communication port 23. With minor adaptation, this port may also be used to communicate with a Compact Flash (CF) card. Adapters to do this are commercially available and are known to those skilled in the art.

First mass storage device 24 can be of the type including a housing and a connector 25 implemented according to the USB standard for passing electronic signaling (and power) to and from the housing. In the present embodiment, however, the storage unit 14 is integrated within a single housing including the protection module. The housing includes first and second local mass storage ports 24, 26 which are sockets designed to mate with CF card 28, 30, respectively, or can include a single socket designed to accept two cards. Both styles are commonly known in the industry and thus not described further here. In addition, a power input port 34 is provided, with a connector that can mate to a spare disk drive power cable 36. This connector supplies operating power to the protection device 10 from a supply connector 38 located on motherboard 12, where the power may be suitably conditioned by an on-board regulator as needed.

Both "read" and "write" operations are necessary to read data from the storage device, and only the type of commands presented during the "write" operations will determine whether the subsequent accesses to the data bus will result in data being read out of the storage device, or whether data will be written

into it in violation of gaming regulations. Accordingly, and unlike conventional memory chips, it is not adequate to merely cut the write line to a Compact Flash Card in order to write-protect it.

Sitting between the IDE port 20 and the CF ports 24, 26 is a protection module 11 comprising in a preferred embodiment a field-programmable gate array (FPGA) containing the logical implementation of the device. In the preferred embodiment, this FPGA is a device which stores its programming internally, without an external programming device as is common to some types of FPGAs. Such FPGAs can be secured so that their contents cannot be read out after programming to make it much more difficult to attack the encryption algorithm or keys contained inside.

Within the FPGA, various operations take place which implement the details of the invention. These operations are performed based on pre-programmed patterns loaded into the FPGA when the protection device is manufactured. This is similar to the programming process for a microcontroller, but the FPGA implements logic instead of executing sequential instructions. Unlike a microcontroller, the response time of the FPGA to an external stimulus is limited only by the propagation time across the device, not by a quantity of clocked execution cycles. Thus, the time for the protection device to perform its function is measured in nanoseconds, instead of the microseconds-to-milliseconds that a microcontroller may require.

This is important because access to the stored data in the CF card will be delayed by the time necessary to qualify the instructions requesting that data.

The IDE interface 20 presents commands and data to CF card or cards 28, 30 using the 16 bit data bus and some control signals. Most important of these are the /READ and /WRITE signals, active-low strobes which indicate the presence of valid data on the bus 22. Two chip select signals (/CS1 and /CS2) indicate whether the data presented is a command to set up the card for a data operation, or the data to be read from or written to the CF card. The methods of using this interface are generally known as the ATA and ATAPI standards, and are documented by an ANSI standard referenced above.

The FPGA protection device includes an identifier module 40 and a comparator module 42. Attention will now be directed to comparator module 42 and also to the flow diagram illustrated in FIG. 2. Commands are forwarded in block 100 from IDE port 20 on motherboard 12, through line 22 to a compact flash card 28 coupled to CF reader 14. The command is intercepted by protection device 10 in block 102 and passed through com port 18 to comparator module 42 and identifier 40. Every time the /WRITE signal is detected in block 104, the command and data bus information is latched in block 106 by write logic circuits 44 into a holding register 46 in the FPGA. A lookup is then performed in the FPGA in block 108 to match the command against the list of valid commands 48 allowed for the CF card. Examples of such commands might be setting the current data pointer to the next sector to be read, or loading the number of operations to be performed in an upcoming bulk read operation. These operations require a write cycle to tell the CF card what data is to be accessed, but the write operation does not have the ability to change the data on the card.

If the command matches one of the allowed commands on the approved list as ascertained in block 110, then the contents of the holding register 46 are transferred to the matching signal pins on the CF card 28 in block 112. In an alternate embodiment, the drive select signal illustrated by selector 50 in FIG. 1 may be used to steer the register contents to the appropriate CF card in local mass storage device 24 or through a third communication port 51 to a different mass storage device 26.

In such an embodiment, it may be that the approved list of commands for one of the CF cards would permit write operations, perhaps restricted to a specific region of the card or otherwise constrained by the regulatory needs of the gaming application.

If the command is not one of the approved commands, then the signals on the CF card are held in an idle state in block 114, preventing the non-approved command from ever reaching the card. The protection device may implement a default response indicating command failure, using the error register method in the ATA standard. Alternatively, the protection device may also set a "lock" bit

internally which prevents any subsequent operation at all, and requires a power-down-and-restart of the device to remove the lock.

If a read cycle is asserted (using the /READ strobe) the signals may be passed straight through from block 104 to the appropriate CF card in block 112, since these cycles do not have the ability to alter data on the CF card. Or, as described above, the protection device may choose to block all access while in a fault mode.

Since the protection device essentially "filters" the commands presented by the IDE interface, allowing only a subset of them to pass, it is apparent to those skilled in the art that removal of the protection device would leave the CF card open to alteration while in operation within the gaming machine. The next element of the invention addresses that deficiency.

It is desirable to verify on a periodic basis that the protection device is still present in the gaming machine. In such an application, physical access to the device can be made difficult, by means of locked doors, intrusion detectors, tamper-resistant seals and other such methods well known in the gaming industry. To remove the protection device is therefore not a trivial task, and a simple periodic check of the device's presence is sufficient. The test must not be easily bypassed however, nor should it be simple to emulate using a "fake" protection device such as a hacker might employ.

Various methods using cryptography algorithms are well known in the art. The protection device 10 is equipped with an identifier module 40 implementing one of these algorithms within encryptor block 52, and the protection device responds to a specific command with a sequence of encrypted data using a secret key 54. Referring to FIG. 3, the gaming machine through motherboard 12 presents a data stream A and the protection device responds with encrypted information B that satisfies the identification requirement. Many such methods are known, and many combinations and permutations of them can be used to foil a potential attacker. The command sequence can either be a command like the "identify device" command already documented in the ATA/ATAPI standard, or it can be some unused command from the list of reserved command types.

Numerous undocumented or illegal command codes are available for this purpose, and their use in such a dedicated application poses no interoperability problem.

The present invention does not address the issue of external alteration of the CF card data, by removing the CF card from the protection device and altering it elsewhere. Existing methods and regulations are considered sufficient to deal with this threat, in the same way that an attacker might alter the data stored in an EPROM or programmable microcontroller. The present invention addresses only the in-machine alteration of data on a CF card, and detection of the presence of the protection device in the gaming machine.

A further desirable feature of the invention is the means to determine that it contains the programming which it is purported by the manufacturer to have been programmed with. To this end, a command much like the encryption response command described above may be implemented, which performs an internal check of the protection device programming and reports this value. Such "checksum" or "CRC" methods are well known in the art and commonly used for verification of memory storage devices like EPROMs. Unlike an EPROM, the internal programming is not directly readable, but it may be used to generate an internally calculated value which offers a reasonable assurance that the programming is correct. An extension of this can be to use the calculated value as a seed for the encryption response command described earlier, along with variations and permutations of these methods.

Having described and illustrated the principles of the invention in a preferred embodiment thereof, it should be apparent that the invention can be modified in arrangement and detail without departing from such principles. The protection device disclosed herein is not limited only to use with flash memory technologies but any writable mass storage device such as hard drives. We claim all modifications and variation coming within the spirit and scope of the following claims.

CLAIMS

1. A mass storage data protection device for use with an industry-standard mass storage device and industry standard personal computer disk drive controller, comprising:

a first communication port (18) for connection to a disk drive controller port (20);

a second communication port (23) for connection to a mass storage device (14);

a comparison means (42) in connection with both communication ports (18, 23), wherein commands presented at the first port are matched against a preselected set of approved commands (48);

an output means (112) in connection with the second communication port (23), which activates only for commands meeting the approval test (1 10) from the comparison means (42); and

an output means (40) in connection with the first communication port (18), which responds to selected commands presented at the first communication port, or delivers data presented by the mass storage device (14) on the second communication port (23).

2. The protection device of claim 1, further comprising an encryption means (52) connected to the first communication port (18), together with an internally stored secret key (54), respondent to a challenge presented at the first communication port, responding with an encrypted version of the challenge.

3. The protection device of claim 2, wherein the encryption means (52) uses one of plurality of algorithms, including IDEA, DES, 3-DES, PGP or others, either separately or in combination, with keys of varying lengths.

4. The protection device of claim 1, wherein the comparison means (42) denies subsequent access to the mass storage device (14) if a command is received which is not one of the approved commands.

5. The protection device of claim 1, further comprising a comparison means for generating a unique signature based on the internal program and approved command list, and an output means for presenting this signature at one

or more of the communication ports on receipt of a valid password requesting the signature, for verification of internal programming of the device by regulatory agencies, the manufacturer or others privileged to this information.

6. The protection device of claim 1, further comprising a third communication port (51) connected to a physically separate mass storage device (26), together with a selection means (50) connected to all three communication ports to determine which of the mass storage devices shall be active.

7. The protection device of claim 6, wherein the list of approved commands is unique for each of the mass storage devices.

8. The protection device of claim 7, further comprising an encryption means (52) connected to the first communication port (18), together with an internally stored secret key (54), respondent to a challenge presented at the first communication port, responding with an encrypted version of the challenge.

9. The protection device of claim 8, wherein the encryption means (52) uses one of plurality of algorithms, including IDEA, DES, 3-DES, PGP or others, either separately or in combination, with keys of varying lengths.

10. The protection device of claim 7, wherein the comparison means (42) denies subsequent access to the mass storage device (14) if a command is received which is not one of the approved commands.

11. The protection device of claim 7, further comprising a comparison means for generating a unique signature based on the internal program and approved command list, and an output means for presenting this signature at one or more of the communication ports on receipt of a valid password requesting the signature, for verification of internal programming of the device by regulatory agencies, the manufacturer or others privileged to this information.

12. A gaming machine comprising;

a housing;

at least one user input coupled to the housing; and

a disk controller;

a mass storage device for storing program code for the gaming machine; and the protection device of claim 1.

13. The gaming machine of claim 12, further comprising an encryption and decryption means communicative with the protection device and containing keys suitable for generating or decoding encrypted communications with said protection device.

14. A data protection device adapted to be interposed between a motherboard and a mass storage device, the data protection device comprising:

an identifier module operatively coupled to an IDE port on a motherboard and including an encryptor capable of implementing a cryptography algorithm using secret key on a data stream received from the motherboard; and

a comparator module including write logic capable of passing only those commands received from the motherboard to the mass storage device that are indicated in a valid command list associated with the write logic, otherwise passing an invalid command received by the protection device into a holding register without passing the invalid command to the mass storage device.

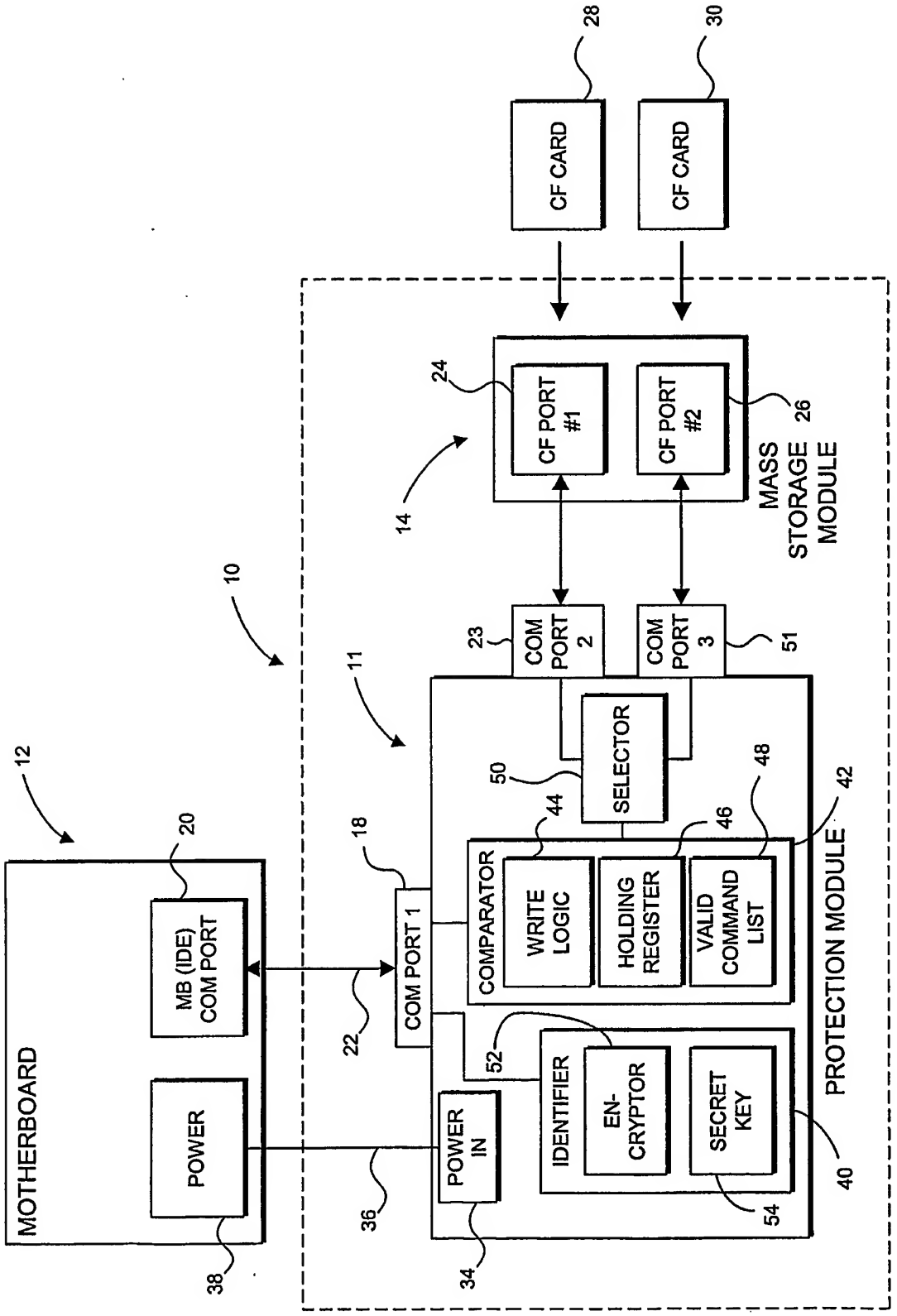

CF CARD
CF CARD
28
30
24
CF PORT #1
CF PORT #2
26
MASS STORAGE MODULE
14
10
11
23
COM PORT 2
COM PORT 3
51
12
20
18
50
SELECTOR
44
46
48
42
COMPARATOR
WRITE LOGIC
HOLDING REGISTER
VALID COMMAND LIST
MB (IDE) COM PORT
COM PORT 1
22
52
IDENTIFIER
EN-CRYPTOR
SECRET KEY
PROTECTION MODULE
MOTHERBOARD
POWER
POWER IN
36
34
38
40
54

FIG. 1

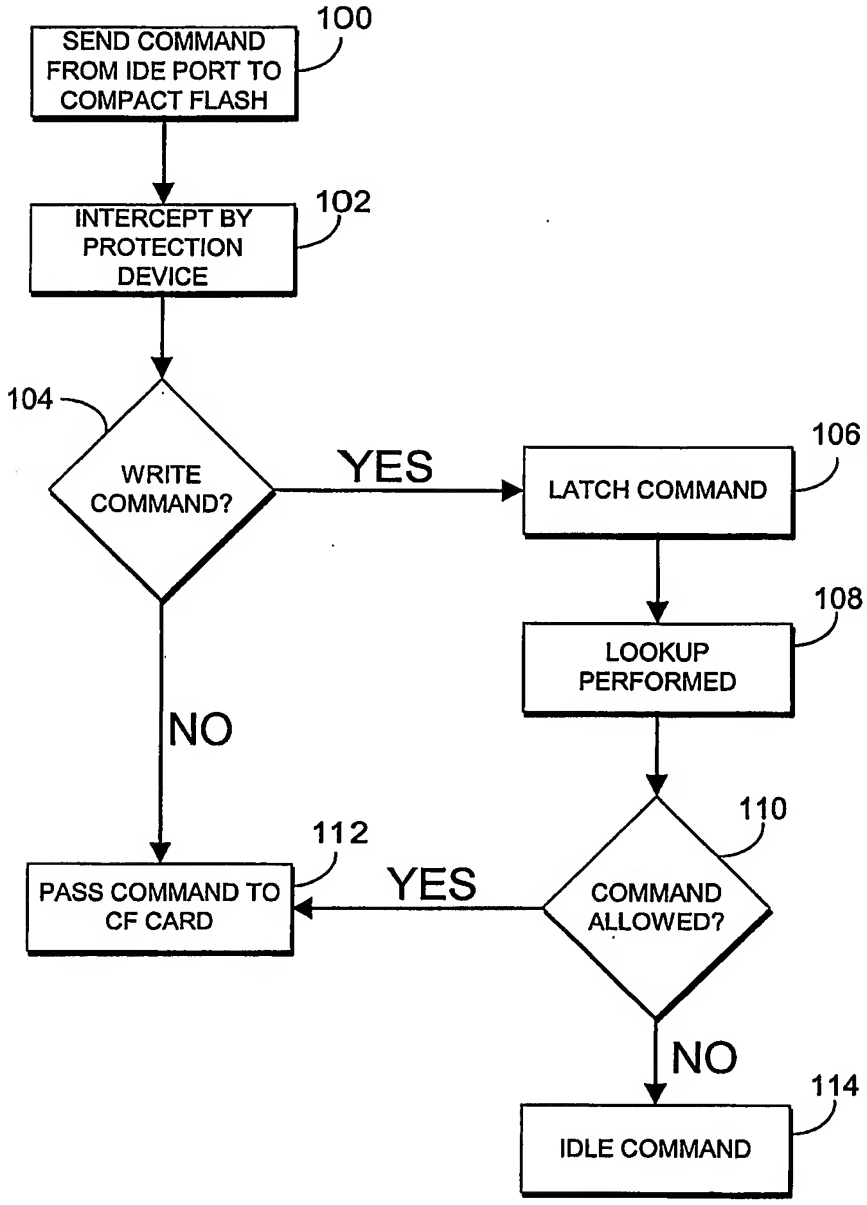

SEND COMMAND FROM IDE PORT TO COMPACT FLASH
100
INTERCEPT BY PROTECTION DEVICE
102
104
WRITE COMMAND?
YES
LATCH COMMAND
106
LOOKUP PERFORMED
108
NO
110
COMMAND ALLOWED?
112
YES
PASS COMMAND TO CF CARD
NO
IDLE COMMAND
114

FIG. 2

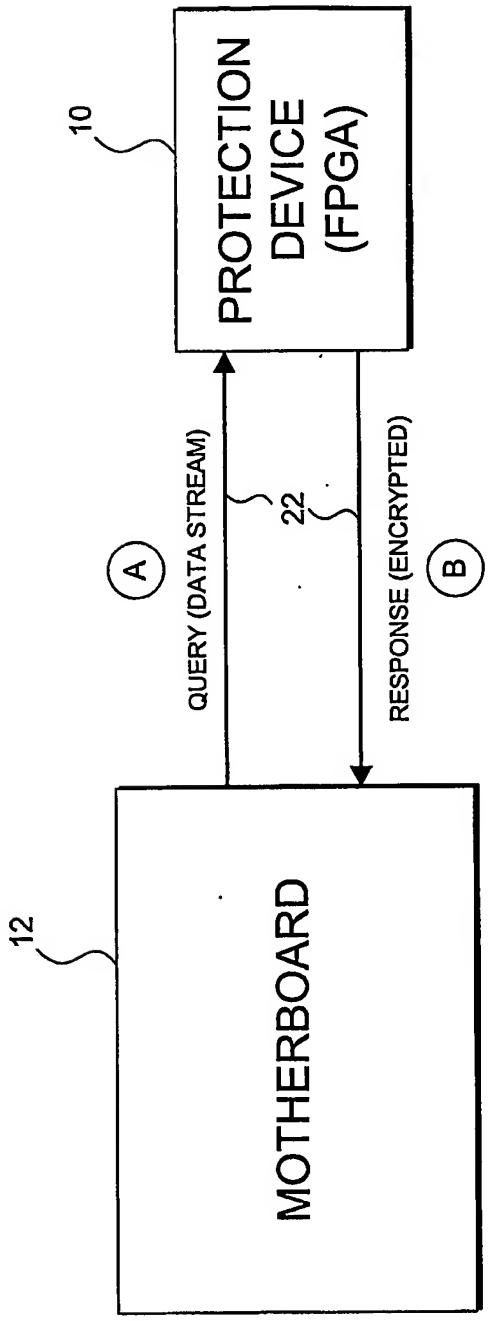

PROTECTION DEVICE (FPGA)
10
QUERY (DATA STREAM)
22
RESPONSE (ENCRYPTED)
A
B
MOTHERBOARD
12

FIG. 3